United States Court of Appeals
For the First Circuit

No. 16-1567

UNITED STATES OF AMERICA,

Appellant,

v.

ALEX LEVIN,

Defendant, Appellee.

APPEAL FROM THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MASSACHUSETTS

[Hon. William G. Young, U.S. District Judge]

Before
Torruella, Selya, and Lynch,
Circuit Judges.

Kelly Begg Lawrence, Assistant United States Attorney, with whom Carmen M. Ortiz, United States Attorney, was on brief, for appellant.

J. W. Carney, Jr., with whom Nathaniel Dolcort-Silver and J. W. Carney, Jr. & Associates were on brief, for appellee.

Mark Rumold, with whom Andrew Crocker, Electronic Frontier Foundation, Jessie J. Rossman and American Civil Liberties Union of Massachusetts, were on brief, as amici curiae.

Caroline Wilson Palow, Scarlet Kim and Privacy International on brief, as amici curiae.

October 27, 2017

TORRUELLA, **Circuit Judge**. Central to this case is the Federal Bureau of Investigation's ("FBI" or "government") use of software that it terms a Network Investigative Technique ("NIT"). The FBI used the NIT pursuant to a warrant it obtained from a magistrate judge in the Eastern District of Virginia (the "NIT warrant"). The FBI installed the NIT on Playpen, a child pornography website it had taken over and was operating out of Virginia. The NIT attached itself to anything that was downloaded from Playpen, and thus effectively travelled to the computers that were downloading from the website, regardless of where those computers were located. The NIT then caused those computers to transmit several specific items of information -- which would allow the FBI to locate the computers -- back to the FBI.

One computer the FBI located in this manner belonged to Alex Levin of Norwood, Massachusetts. After a search of his computer pursuant to a subsequent search warrant issued in Massachusetts, the FBI found various media files allegedly containing child pornography. Levin was indicted and charged with one count of possession of child pornography, in violation of 18 U.S.C. § 2252A(a)(5)(B). Levin moved to suppress the evidence seized pursuant to the NIT warrant and the warrant issued in Massachusetts. The district court granted suppression, United States v. Levin, 186 F. Supp. 3d 26, 44 (D. Mass. 2016), and the government appealed. We disagree with the district court that suppression is warranted, because the FBI acted in good faith reliance on the NIT warrant. Accordingly, we vacate the district court's suppression order and remand for further proceedings.[1]

I. Background

A. Playpen and the Dark Web

Child-pornography websites are a source of significant social harm. "[T]he exploitive use of children in the production of pornography" was already "a serious national problem" decades ago. New York v. Ferber, 458 U.S. 747, 749 (1982). Modern technology, which allows images and videos to be "traded with ease on the [i]nternet," has only amplified the problem. Paroline v. United States, 134 S. Ct. 1710, 1717 (2014). The child-pornography website at the center of this case -- and several dozen other cases throughout the nation[2] -- bore the name "Playpen."

[1] Recently, both the Eighth and Tenth Circuit reached similar results in two cases involving the execution of the same NIT warrant at issue in this appeal. See United States v. Horton, 863 F.3d 1041 (8th Cir. 2017) (reversing the district court's order suppressing evidence obtained through the NIT warrant, pursuant to the Leon good-faith exception, even though it determined that the NIT was void ab initio because the magistrate judge exceeded her jurisdiction under Rule 41(b)); United States v. Workman, 863 F.3d 1313 (10th Cir. 2017) (reversing the district court's order suppressing evidence obtained through the NIT warrant, pursuant to the Leon good-faith exception, without deciding if the magistrate judge lacked the authority to issue the NIT warrant).

[2] See, e.g., United States v. Taylor, No. 2:16-cr-00203-KOB-JEO-1, 2017 WL 1437511, at *3-4 (N.D. Ala. Apr. 24, 2017) (collecting

Playpen attracted web traffic on a massive scale. Just between August 2014 and February 2015, more than 150,000 users accessed the site. Visitors to Playpen made over 95,000 posts on over 9,000 topics, all pertaining to child pornography. Playpen also featured discussion forums where its users discussed issues such as how to groom child victims and how to evade law enforcement.

Playpen operated on the internet network known as Tor (short for "The Onion Router"). This network, together with similar networks, is known as the Dark Web. The United States Naval Research Laboratory originally created Tor as a means of protecting government communications. Today, however, the Tor network is publicly accessible. One gains access to the Tor network by downloading the Tor software. By masking its users' actual IP addresses -- which could otherwise be used to identify users -- that software offers its users much greater anonymity than do conventional web browsers. Tor achieves this masking by bouncing users' communications around a distributed network of relay computers run by volunteers all around the world. The Tor software can be used to access the conventional internet as well as the Dark Web.

and categorizing cases).

Websites on the Dark Web, known as hidden services, can be reached only by using Tor software, or a similar software. Playpen was one such hidden service. Unlike websites on the conventional internet, hidden services cannot be accessed through public search engines such as Google. Hidden services can be accessed by using their addresses, if known to the person seeking to access the hidden service, or by being redirected to them. The latter can occur when, for instance, a link to a hidden service is posted on another hidden service and a user clicks that link.

Because Playpen was a hidden service, a Playpen user had to take several affirmative steps to access the site. First, he or she needed to download and install the Tor software. Second, the user would need to acquire the unique web address for Playpen. Third, the user would use this address to find Playpen in the Tor Network. And finally, he or she needed to enter a username and password on Playpen's main page to access the site's content. The main page displayed "two images depicting partially clothed prepubescent females with their legs spread apart." Thus, Playpen's subject matter was obvious even before the user logged in and accessed the child-pornography content.

B. The Warrants and the NIT

In February 2015, FBI agents seized control of Playpen pursuant to a warrant (which is not at issue in the present case).

After seizing control, the FBI continued to run Playpen out of a government facility in the Eastern District of Virginia for two weeks, with the purpose of identifying and apprehending Playpen users.

On February 20, 2015, the government obtained the NIT warrant from a magistrate judge in the Eastern District of Virginia. This warrant permitted the FBI to install the NIT on its server that hosted Playpen, and thereby to obtain information from "[t]he activating computers [which] are those of any user or administrator who logs into [Playpen] by entering a username and password." The warrant authorized the FBI to obtain seven items of information: (1) the activating computer's actual IP address, and the date and time that the NIT determines what the IP address is; (2) a unique identifier generated by the NIT (e.g., a series of numbers, letters, and/or special characters) to distinguish data from that of other activating computers, that will be sent with and collected by the NIT; (3) the type of operating system running on the computer, including type (e.g., Windows), version (e.g., Windows 7), and architecture (e.g., x 86); (4) information about whether the NIT has already been delivered to the activating computer; (5) the activating computer's Host Name; (6) the activating computer's active operating system username; and (7) the activating computer's media access control ("MAC") address.

Case 1:15-cr-10271-WGY Document 111 Filed 10/27/17 Page 7 of 16

After the NIT was installed on the government's server, it worked in two steps. First, it augmented the content of the website with additional computer instructions. Once a user or administrator who had logged into Playpen downloaded such content, he or she would also download those additional computer instructions, which comprise the NIT. Then, the NIT would cause the activating computer to transmit the seven pieces of information, described above and authorized to be obtained by the warrant, back to a computer controlled by the FBI. The NIT did not deny the user of the activating computer access to any data or functionality of its computer. The NIT allowed the FBI to identify the IP addresses of hundreds of Playpen users around the country, including in the Eastern District of Virginia.

Using the NIT, the government determined that a Playpen user named "Manakaralupa" had accessed several images of child pornography in early March 2015. The NIT caused Manakaralupa's activating computer to transmit the aforementioned information to the government. Using the seized information, the government traced the IP address of that user to Levin's home address in Norwood, Massachusetts.

On August 11, 2015, the government obtained a warrant from a magistrate judge in the District of Massachusetts to search Levin's home. The government executed the warrant the next day, searched Levin's computer, and identified eight media files allegedly containing child pornography.

On September 17, 2015, Levin was indicted and charged with one count of possession of child pornography, in violation of 18 U.S.C. § 2252A(a)(5)(B). After Levin moved to suppress all evidence seized pursuant to the NIT warrant and the warrant authorizing the search of his home, the district court granted Levin's motion on May 5, 2016. First, the district court found that, since the warrant purported to authorize a search of property located outside the federal judicial district where the issuing judge sat, the NIT warrant was issued without jurisdiction and thus was void ab initio. The court reasoned that the magistrate judge was not authorized to issue it either under Rule 41 of the Federal Rules of Criminal Procedure[3] or under the Federal

[3] Rule 41 has been amended, apparently specifically to permit magistrate judges to issue warrants such as the NIT warrant. It now reads:

> [A] magistrate judge with authority in any district where activities related to a crime may have occurred has authority to issue a warrant to use remote access to search electronic storage media and to seize or copy electronically stored information located within or outside that district if: (A) the district where the media or information is located has been concealed through technological means . . . .

Fed. R. Crim. P. 41(b)(6).

Because this amendment became effective on December 1, 2016, however, it does not apply to the present case. United States v.

Magistrates Act, 28 U.S.C. § 636(a).[4]

Second, the district court determined that suppression was an appropriate remedy because the violation of Rule 41 was substantive, rather than technical. The court reasoned that, since the magistrate judge did not have jurisdiction to issue the warrant, there was no judicial approval. According to the district court, the resulting search was thus conducted as if not pursuant to any warrant authorization, and was therefore presumptively unreasonable.

The district court further concluded that, even if that error were technical, suppression would still be appropriate, as Levin demonstrated that he suffered prejudice. The court reasoned that, had Rule 41(b) been followed, the magistrate judge would not have issued the NIT warrant, and, therefore, the search conducted pursuant thereto might not have occurred. Finally, the court

Walker-Couvertier, 860 F.3d 1, 9 (1st Cir. 2017).

[4] Section 636(a) of the Federal Magistrates Act reads:

> Each United States magistrate judge . . . shall have within the district in which sessions are held by the court that appointed the magistrate judge, at other places where that court may function, and elsewhere as authorized by law--(1) all powers and duties conferred or imposed upon United States commissioners by law or by the Rules of Criminal Procedure for the United States District Courts . . . .

Id.

opined that the good-faith exception did not apply because the search was conducted pursuant to a warrant that, in its view, was void ab initio.

II. Discussion

"[W]hen considering a suppression ruling, we review legal questions de novo and factual findings for clear error." United States v. Ponzo, 853 F.3d 558, 572 (1st Cir. 2017). We disagree with the district court's ruling suppressing the evidence seized pursuant to the NIT warrant. Regardless of whether a Fourth Amendment violation occurred, the facts of this case show that the Leon good-faith exception applies.

"The Fourth Amendment contains no provision expressly precluding the use of evidence obtained in violation" of its terms. United States v. Leon, 468 U.S. 897, 906 (1984). Nevertheless, the Supreme Court created the exclusionary rule as a "'prudential' doctrine . . . 'to compel respect for the constitutional guaranty.'" Davis v. United States, 564 U.S. 229, 236 (2011) (first quoting Pa. Bd. of Prob. & Parole v. Scott, 524 U.S. 357, 363 (1998); and then quoting Elkins v. United States, 364 U.S. 206, 217 (1960)). The exclusion of evidence obtained by an unconstitutional search is "not a personal constitutional right" but a remedy whose "sole purpose . . . is to deter future Fourth

Amendment violations." Id. at 236-37 (quoting Stone v. Powell, 428 U.S. 465, 486 (1976)).

Under the exclusionary rule, courts may suppress evidence "obtained as a direct result of an illegal search or seizure" as well as evidence that is the "fruit of the poisonous tree." Utah v. Strieff, 136 S. Ct. 2056, 2061 (2016) (quoting Segura v. United States, 468 U.S. 796, 804 (1984)). However, due to the significant costs of suppressing evidence of crimes, the exclusionary rule applies "only . . . where its deterrence benefits outweigh its substantial social costs." Id. (quoting Hudson v. Michigan, 547 U.S. 586, 591 (2006)) (alteration in original). "[T]he deterrence benefits of exclusion 'var[y] with the culpability of the law enforcement conduct' at issue. When the police exhibit 'deliberate,' 'reckless,' or 'grossly negligent' disregard for Fourth Amendment rights, the deterrent value of exclusion is strong and tends to outweigh the resulting costs." Davis, 564 U.S. at 238 (quoting Herring v. United States, 555 U.S. 135, 143-44 (2009) (second alteration in original). However, "when the police act with an objectively reasonable good-faith belief that their conduct is lawful . . . or when their conduct involves only simple, isolated negligence . . . the deterrence rationale loses much of its force, and exclusion cannot pay its way." Id. (internal citations and quotation marks omitted).

The Supreme Court has clearly delineated the bounds of the good faith exception. Suppression remains appropriate:

> 1. "[I]f the magistrate or judge in issuing a warrant was misled by information in an affidavit that the affiant knew was false or would have known was false except for his reckless disregard of the truth."
> 2. "[W]here the issuing magistrate wholly abandoned his judicial role."
> 3. Where the executing officer relies "on a warrant based on an affidavit 'so lacking in indicia of probable cause as to render official belief in its existence entirely unreasonable.'"

Leon, 468 U.S. at 923 (citations omitted).

Furthermore, "[t]he Leon good faith exception does not apply where . . . a warrant . . . is 'so facially deficient--i.e. in failing to particularize the place to be searched or the things to be seized--that the executing officers cannot reasonably presume it to be valid.'" United States v. Woodbury, 511 F.3d 93, 99 (1st Cir. 2007) (citing United States v. Owens, 167 F.3d 739, 475 (1st Cir. 1999)).

Finally, in determining whether a reasonable officer should have known that a search was illegal despite a magistrate's authorization, "a court must evaluate all the attendant circumstances, keeping in mind that Leon requires . . . objective good faith." United States v. Ricciardelli, 998 F.2d 8, 15 (1st Cir. 1993) (internal citations omitted).

None of the four conditions identified by Leon apply. Levin argues that the NIT warrant was akin to a general warrant and therefore so obviously lacking in particularity that the officers' reliance on it amounted to bad faith. *See* *United States* v. *Ninety-Two Thousand Four Hundred Twenty-Two Dollars & Fifty-Seven Cents*, 307 F.3d 137, 149 (3d Cir. 2002) (Alito, J.) (distinguishing between an "overly broad" warrant, under which evidence "need not be suppressed if the good faith exception applies," and a warrant that is so "general" that "executing officers could not have reasonably trusted in its legality"). A plain reading of the NIT warrant, however, shows otherwise. "The general warrant specified only an offense . . . and left to the discretion of the executing officials the decision as to which persons should be arrested and which places should be searched." *Steagald* v. *United States*, 451 U.S. 204, 220 (1981). In the case at hand, in contrast, the NIT warrant did not leave to the discretion of the executing officials which places should be searched, because the NIT warrant clearly specifies that only activating computers -- that is "those of any user . . . who logs into [Playpen] by entering a username and password" -- are to be searched. The NIT warrant specifies into which homes an intrusion is permitted (those where the activating computers are located), and on what basis (that the users in those homes logged into Playpen). And if the government wished to conduct any further searches of anyone's home, it would have needed obtain an additional warrant -- which is exactly what it did in this case. Therefore, the NIT warrant "was not so facially deficient that the executing officers could not reasonably have presumed it to be valid." Woodbury, 511 F.3d at 100.

We are unpersuaded by Levin's argument that because, at least according to him, the government was not sure whether the NIT warrant could validly issue under Rule 41, there is government conduct here to deter. Faced with the novel question of whether an NIT warrant can issue -- for which there was no precedent on point -- the government turned to the courts for guidance. The government presented the magistrate judge with a request for a warrant, containing a detailed affidavit from an experienced officer, describing in detail its investigation, including how the NIT works, which places were to be searched, and which information was to be seized.[5] We see no benefit in deterring such conduct -- if anything, such conduct should be encouraged, because it leaves it to the courts to resolve novel legal issues.[6]

[5] Although Levin protests that the warrant failed to describe the activating computers as the places to be searched, the request for a warrant in fact, under the heading "Place to be Searched," states that the NIT will obtain "information . . . from the activating computers described below." The request for the warrant goes on to explain that "[t]he activating computers are those of any user or administrator who logs into [Playpen] by entering a username and password."

[6] This situation is, of course, distinct from one in which the government would request and somehow obtain a warrant for conduct

Thus, we are unpersuaded that there was any bad faith on the part of the executing officers. The officers acted pursuant to the warrant. To the extent that a mistake was made in issuing the warrant, it was made by the magistrate judge, not by the executing officers, and the executing officers had no reason to suppose that a mistake had been made and the warrant was invalid. As discussed above, the NIT warrant was not written in general terms that would have signaled to a reasonable officer that something was amiss. The warrant in this case was particular enough to infer that, in executing it, "the [executing officers] act[ed] with an objectively 'reasonable good-faith belief' that their conduct [was] lawful." Davis, 564 U.S. at 238. Under these circumstances, "the 'deterrence rationale loses much of its force,' and exclusion cannot 'pay its way.'" Id. (internal citations omitted).[7]

Therefore, because the government acted in good faith reliance on the NIT warrant, and because the deterrent effects on law enforcement do not outweigh the great cost to society of suppressing the resulting evidence, suppression is not warranted.

it knows to be illegal.

[7] Any deterrent effect is further limited by the fact that Rule 41 has been amended and now appears to allow a magistrate to issue NIT warrants such as the one at issue here. See supra note 3.

III. Conclusion

The district court erred in granting the motion to suppress. Because the executing officers acted in good faith reliance on the NIT warrant, the Leon exception applies. Accordingly, the district court's order is vacated, and the case is remanded for further proceedings not inconsistent with this opinion.

Vacated and Remanded.